Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1-42. (canceled)

43. (Currently Amended) A ~~processor for performing multiplication~~ programmable CPU multiplier responsive to instructions dedicated to polynomial operations, comprising:

a first array that is used to perform arithmetic multiplication, the first array having a first result output and a second result output;

a second array that is used to perform binary polynomial multiplication, the second array having a third result output; and

a carry propagation adder having a first input, a second input, and an output, wherein

the first input of the carry propagation adder is selectively coupled to the first result output of the first array,

the second input of the carry propagation adder is selectively coupled to the second result output of the first array and the third result output of the second array, and

the output of the carry propagation adder is stored in a register to provide an output of the polynomial operations.

44. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, further comprising:

a first multiplexer coupled to the first result output of the first array;

a first register coupled between an output of the first multiplexer and the first input of the carry propagation adder;

a second multiplexer coupled to the second result output of the first array; and

a second register coupled between an output of the second multiplexer and the second input of the carry propagation adder.

45. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 44, wherein the third result output of the second array is coupled to an input of the second multiplexer.

46. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 44, wherein an output of the first register is coupled to an input of the first array and an input of the second array.

47. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 44, wherein an output of the second register is coupled to an input of the first array.

48. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the first array includes a plurality of carry-save adders arranged in a tree structure.

49. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the first array is a Wallace tree multiplier array.

50. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the first array is a 32-bit by 16-bit array.

51. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the second array is a 32-bit by 16-bit array.

52. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the processor performs 32-bit by 32-bit multiplications.

53. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the processor multiplies a first operand and a second operand to form a resultant value, the first operand being provided to a first input of the first array and the second operand being provided to a second input of the first array, and wherein the resultant value is available at an output of the carry propagation adder.

54. (Currently Amended) The ~~processor~~ programmable CPU multiplier of claim 43, wherein the processor multiplies a first polynomial value and a second polynomial value to form a resultant value, the first polynomial value being provided to a first input of the second array and the second polynomial value being provided to a second input of the second array, and wherein the resultant value is available at an output of the carry propagation adder.

55. (Currently Amended) A tangible computer-readable storage medium comprising a ~~processor for performing multiplication~~ programmable CPU multiplier responsive to instructions dedicated to polynomial operations embodied in software, the ~~processor~~ programmable CPU multiplier comprising:

a first array that is used to perform arithmetic multiplication, the first array having a first result output and a second result output;

a second array that is used to perform binary polynomial multiplication, the second array having a third result output; and

a carry propagation adder having a first input, a second input, and an output, wherein

the first input of the carry propagation adder is selectively coupled to the first result output of the first array,

the second input of the carry propagation adder is selectively coupled to the second result output of the first array and the third result output of the second array, and

the output of the carry propagation adder is stored in a register to provide an output of the polynomial operations.

56. (Currently Amended) The tangible computer-readable storage medium of claim 55, wherein the ~~processor~~ programmable CPU multiplier embodied in software further comprises:

a first multiplexer coupled to the first result output of the first array;

a first register coupled between an output of the first multiplexer and the first input of the carry propagation adder;

a second multiplexer coupled to the second result output of the first array; and

a second register coupled between an output of the second multiplexer and the second input of the carry propagation adder.

57. (Previously Presented) The tangible computer-readable storage medium of claim 56, wherein the third result output of the second array is coupled to an input of the second multiplexer.

58. (Previously Presented) The tangible computer-readable storage medium of claim 57, wherein an output of the first register is coupled to an input of the first array and an input of the second array.

59. (Previously Presented) The tangible computer-readable storage medium of claim 57, wherein an output of the second register is coupled to an input of the first array.

60. (Previously Presented) The tangible computer-readable storage medium of claim 55, wherein the first array includes a plurality of carry-save adders arranged in a tree structure.

61. (Previously Presented) The tangible computer-readable storage medium of claim 55, wherein the first array is a Wallace tree multiplier array.

62. (Previously Presented) The tangible computer-readable storage medium of claim 55, wherein the first array is a 32-bit by 16-bit array.

63. (Previously Presented) The tangible computer-readable storage medium of claim 55, wherein the second array is a 32-bit by 16-bit array.

64. (Currently Amended) The tangible computer-readable storage medium of claim 55, wherein the ~~processor~~ programmable CPU multiplier performs 32-bit by 32-bit multiplications.

65. (Currently Amended) The tangible computer-readable storage medium of claim 55, wherein the ~~processor~~ programmable CPU multiplier multiplies a first operand and a second operand to form a resultant value, the first operand being provided to a first input of the first array and the second operand being provided to a second input of the first array, and wherein the resultant value is available at an output of the carry propagation adder.

66. (Currently Amended) The tangible computer-readable storage medium of claim 55, wherein the ~~processor~~ programmable CPU multiplier multiplies a first polynomial value and a second polynomial value to form a resultant value, the first polynomial value being provided to a first input of the second array and the second polynomial value being provided to a second input of the second array, and wherein the resultant value is available at an output of the carry propagation adder.

67. (Currently Amended) The tangible computer-readable storage medium of claim 55, wherein the ~~processor~~ programmable CPU multiplier is embodied in hardware description language software.

68. (Currently Amended) The tangible computer-readable storage medium of claim 55, wherein the ~~processor~~ programmable CPU multiplier is embodied in one of

Verilog hardware description language software and VHDL hardware description language software.

69. (Currently Amended) A system, comprising:

a processor for performing multiplication that includes

an execution unit,

a multiply-divide unit, responsive to instructions dedicated to polynomial operations the multiply-divide unit comprising:

a first array that is used to perform arithmetic multiplication, the first array having a first result output and a second result output,

a second array that is used to perform binary polynomial multiplication, the second array having a third result output, and

a carry propagation adder having a first input, a second input, and an output, wherein

the first input of the carry propagation adder is selectively coupled to the first result output of the first array,

the second input of the carry propagation adder is selectively coupled to the second result output of the first array and the third result output of the second array, and

the output of the carry propagation adder is stored in a register to provide an output of the polynomial operations; and

a memory coupled to the processor.

70. (Previously Presented) The system of claim 69, wherein the multiply-divide unit further comprises:

a first multiplexer coupled to the first result output of the first array;

a first register coupled between an output of the first multiplexer and the first input of the carry propagation adder;

a second multiplexer coupled to the second result output of the first array; and

a second register coupled between an output of the second multiplexer and the second input of the carry propagation adder.

71. (Previously Presented) The system of claim 70, wherein the third result output of the second array is coupled to an input of the second multiplexer.

72. (Previously Presented) The system of claim 71, wherein an output of the first register is coupled to an input of the first array and an input of the second array.

73. (Previously Presented) The system of claim 71, wherein an output of the second register is coupled to an input of the first array.

74. (Previously Presented) The system of claim 69, wherein the first array includes a plurality of carry-save adders arranged in a tree structure.

75. (Previously Presented) The system of claim 69, wherein the first array is a Wallace tree multiplier array.

76. (Previously Presented) The system of claim 69, wherein the first array is a 32-bit by 16-bit array.

77. (Previously Presented) The system of claim 69, wherein the second array is a 32-bit by 16-bit array.

78. (Previously Presented) The system of claim 69, wherein the multiply-divide unit performs 32-bit by 32-bit multiplications.

79. (Previously Presented) The system of claim 69, wherein the multiply-divide unit multiplies a first operand and a second operand to form a resultant value, the

first operand being provided to a first input of the first array and the second operand being provided to a second input of the first array, and wherein the resultant value is available at an output of the carry propagation adder.

80. (Previously Presented) The system of claim 69, wherein the multiply-divide unit multiplies a first polynomial value and a second polynomial value to form a resultant value, the first polynomial value being provided to a first input of the second array and the second polynomial value being provided to a second input of the second array, and wherein the resultant value is available at an output of the carry propagation adder.

81. (Previously Presented) The system of claim 69, wherein operation of the multiply-divide unit is decoupled from operation of the execution unit.